Building Distributed Services in an Alliance

Robert Burgess
April 30, 2009
Alliances

Multiple autonomous organizations

Connected by WAN

Mutual benefit to cooperation

Mutual mistrust

Misconfiguration

Failures

Attacks
Alliances

Multiple autonomous organizations

Connected by WAN

Mutual benefit to cooperation

Mutual mistrust

Misconfiguration

Failures

Attacks
Alliances

Multiple autonomous organizations

Connected by WAN

Mutual benefit to cooperation

Mutual mistrust

Misconfiguration

Failures

Attacks
Alliances

Multiple autonomous organizations

Connected by WAN

Mutual benefit to cooperation

Mutual mistrust

Misconfiguration

Failures

Attacks
Alliances

Multiple autonomous organizations

Connected by WAN

Mutual benefit to cooperation

Mutual mistrust

Misconfiguration

Failures

Attacks
Alliances

Multiple autonomous organizations

Connected by WAN

Mutual benefit to cooperation

Mutual mistrust

Misconfiguration

Failures

Attacks
Alliances

Multiple autonomous organizations

Connected by WAN

Mutual benefit to cooperation

Mutual mistrust

Misconfiguration

Failures

Attacks
Alliances

Multiple autonomous organizations

Connected by WAN

Mutual benefit to cooperation

Mutual mistrust

Misconfiguration

Failures

Attacks
Alliances

Byzantine fault tolerance

Threshold signatures

Goals

Library for distributed system-building

In this project, focus on consensus

Generalize threshold signatures

Build higher-level abstractions
Alliances

Byzantine fault tolerance

Threshold signatures

Goals

Library for distributed system-building

In this project, focus on consensus

Generalize threshold signatures

Build higher-level abstractions
Alliances

Byzantine fault tolerance

Threshold signatures

Goals

Library for distributed system-building

In this project, focus on consensus

Generalize threshold signatures

Build higher-level abstractions
Alliances

Byzantine fault tolerance

Threshold signatures

Goals

Library for distributed system-building

In this project, focus on consensus

Generalize threshold signatures

Build higher-level abstractions
Alliances

Byzantine fault tolerance

Threshold signatures

Goals

Library for distributed system-building

In this project, focus on consensus

Generalize threshold signatures

Build higher-level abstractions
Alliances

Byzantine fault tolerance

Threshold signatures

Goals

Library for distributed system-building

In this project, focus on consensus

Generalize threshold signatures

Build higher-level abstractions
Alliances

Byzantine fault tolerance
Threshold signatures

Goals

Library for distributed system-building
In this project, focus on consensus

Generalize threshold signatures

Build higher-level abstractions
Alliances

Byzantine fault tolerance

Threshold signatures

Goals

Library for distributed system-building

In this project, focus on consensus

Generalize threshold signatures

Build higher-level abstractions
Threshold Signatures

asymmetric cryptography

Verifiers hold non-secret public key

1 signatory holds secret private key

Private key $\rightarrow$ signature

$(t, k)$ threshold cryptography

Verifiers are unmodified

$k$ signatories hold private key shares

Private key share $\rightarrow$ signature share

$t$ signature shares $\rightarrow$ signature
Threshold Signatures

asymmetric cryptography

Verifiers hold non-secret public key
1 signatory holds secret private key
Private key $\rightarrow$ signature

$(t, k)$ threshold cryptography
Verifiers are unmodified
$k$ signatories hold private key shares
Private key share $\rightarrow$ signature share
$t$ signature shares $\rightarrow$ signature
Threshold Signatures

asymmetric cryptography

Verifiers hold non-secret public key

1 signatory holds secret private key

Private key $\rightarrow$ signature

$(t, k)$ threshold cryptography

Verifiers are unmodified

$k$ signatories hold private key shares

Private key share $\rightarrow$ signature share

$t$ signature shares $\rightarrow$ signature
Threshold Signatures

asymmetric cryptography

Verifiers hold non-secret public key
1 signatory holds secret private key

Private key $\rightarrow$ signature

$(t, k)$ threshold cryptography

Verifiers are unmodified

$k$ signatories hold private key shares

Private key share $\rightarrow$ signature share

t signature shares $\rightarrow$ signature
Threshold Signatures

asymmetric cryptography

Verifiers hold non-secret public key
1 signatory holds secret private key
Private key $\rightarrow$ signature

$(t, k)$ threshold cryptography

Verifiers are unmodified

$k$ signatories hold private key shares

Private key share $\rightarrow$ signature share

$t$ signature shares $\rightarrow$ signature
Threshold Signatures

asymmetric cryptography

Verifiers hold non-secret public key
1 signatory holds secret private key

Private key $\rightarrow$ signature

$(t, k)$ threshold cryptography

Verifiers are unmodified

$k$ signatories hold private key shares

Private key share $\rightarrow$ signature share

$t$ signature shares $\rightarrow$ signature
Threshold Signatures

asymmetric cryptography

Verifiers hold non-secret public key
1 signatory holds secret private key

Private key → signature

$(t, k)$ threshold cryptography

Verifiers are unmodified

$k$ signatories hold private key shares

Private key share → signature share

t signature shares → signature
Threshold Signatures

asymmetric cryptography

Verifiers hold non-secret public key
1 signatory holds secret private key

Private key $\rightarrow$ signature

$(t, k)$ threshold cryptography

Verifiers are unmodified

$k$ signatories hold private key shares

Private key share $\rightarrow$ signature share

$t$ signature shares $\rightarrow$ signature
Threshold Signatures

asymmetric cryptography

Verifiers hold non-secret public key
1 signatory holds secret private key
Private key → signature

(t, k) threshold cryptography
Verifiers are unmodified
k signatories hold private key shares
Private key share → signature share

t signature shares → signature
Threshold Signatures

asymmetric cryptography

Verifiers hold non-secret public key
1 signatory holds secret private key

Private key → signature

(t, k) threshold cryptography

Verifiers are unmodified

k signatories hold private key shares

Private key share → signature share

t signature shares → signature
Threshold Signatures

RSA scheme by Victor Shoup

Non-interactive operations

Constant share size

Verifiable signature shares

Rigorous security proof
(random oracle)

LaGrange interpolation within RSA exponent
Threshold Signatures

RSA scheme by Victor Shoup

Non-interactive operations

Constant share size

Verifiable signature shares

Rigorous security proof
(random oracle)

LaGrange interpolation within RSA exponent
Threshold Signatures

RSA scheme by Victor Shoup

Non-interactive operations

Constant share size

Verifiable signature shares

Rigorous security proof (random oracle)

LaGrange interpolation within RSA exponent
Threshold Signatures

RSA scheme by Victor Shoup

Non-interactive operations

Constant share size

Verifiable signature shares

Rigorous security proof
(random oracle)

LaGrange interpolation within RSA exponent
Threshold Signatures

RSA scheme by Victor Shoup

Non-interactive operations

Constant share size

Verifiable signature shares

Rigorous security proof
(random oracle)

LaGrange interpolation within RSA exponent
Threshold Signatures

RSA scheme by Victor Shoup

Non-interactive operations

Constant share size

Verifiable signature shares

Rigorous security proof
(random oracle)

LaGrange interpolation within RSA exponent
Threshold Signatures

RSA scheme by Victor Shoup

Non-interactive operations

Constant share size

Verifiable signature shares

Rigorous security proof (random oracle)

LaGrange interpolation within RSA exponent
Consensus

Also known as agreement

Peers must agree on ordering of events

state machine replication

lock services

broadcast

Paxos scheme by Leslie Lamport
Consensus

Also known as agreement

Peers must agree on ordering of events

state machine replication

lock services

broadcast

Paxos scheme by Leslie Lamport
Consensus

Also known as agreement

Peers must agree on ordering of events

- state machine replication
- lock services
- broadcast

Paxos scheme by Leslie Lamport
Consensus

Also known as agreement

Peers must agree on ordering of events

state machine replication

lock services

broadcast

Paxos scheme by Leslie Lamport
Consensus

Also known as agreement

Peers must agree on ordering of events

state machine replication

lock services

broadcast

Paxos scheme by Leslie Lamport
Consensus

Also known as agreement

Peers must agree on ordering of events

state machine replication

lock services

broadcast

Paxos scheme by Leslie Lamport
Consensus

Also known as agreement

Peers must agree on ordering of events

state machine replication

lock services

broadcast

Paxos scheme by Leslie Lamport
Consensus

Fast Asynchronous Byzantine Paxos (FaB)

fast common case 2-step termination

asynchronous weak network assumptions

byzantine allows mutual mistrust

Depends on cryptographic signatures
Consensus

Fast Asynchronous Byzantine Paxos (FaB)

**fast** common case 2-step termination

**asynchronous** weak network assumptions

**byzantine** allows mutual mistrust

Depends on cryptographic signatures
Consensus

Fast Asynchronous Byzantine Paxos (FaB)

**fast** common case 2-step termination

**asynchronous** weak network assumptions

**byzantine** allows mutual mistrust

Depends on cryptographic signatures
Consensus

Fast Asynchronous Byzantine Paxos (FaB)

**fast** common case 2-step termination

**asynchronous** weak network assumptions

**byzantine** allows mutual mistrust

Depends on cryptographic signatures
Consensus

Fast Asynchronous Byzantine Paxos (FaB)

- **fast** common case 2-step termination
- **asynchronous** weak network assumptions
- **byzantine** allows mutual mistrust

Depends on cryptographic signatures
Consensus

Fast Asynchronous Byzantine Paxos (FaB)

**fast** common case 2-step termination

**asynchronous** weak network assumptions

**byzantine** allows mutual mistrust

Depends on cryptographic signatures
Ally Consensus

FaB Paxos library

With threshold signatures instead of normal

When checking responses from a quorum, combine

Enables tolerance of failures without key revocation

Generalizing threshold cryptography, enables arbitrary definitions of quorums
Ally Consensus

FaB Paxos library

With threshold signatures instead of normal

When checking responses from a quorum, combine

Enables tolerance of failures without key revocation

Generalizing threshold cryptography, enables arbitrary definitions of quorums
Ally Consensus

FaB Paxos library

With threshold signatures instead of normal

When checking responses from a quorum, combine

Enables tolerance of failures without key revocation

Generalizing threshold cryptography, enables arbitrary definitions of quorums
Ally Consensus

FaB Paxos library

With threshold signatures instead of normal

When checking responses from a quorum, combine

Enables tolerance of failures without key revocation

Generalizing threshold cryptography, enables arbitrary definitions of quorums
Ally Consensus

FaB Paxos library

With threshold signatures instead of normal

When checking responses from a quorum, combine

Enables tolerance of failures without key revocation

Generalizing threshold cryptography, enables arbitrary definitions of quorums
Ally Consensus

FaB Paxos library

With threshold signatures instead of normal

When checking responses from a quorum, combine

Enables tolerance of failures without key revocation

Generalizing threshold cryptography, enables arbitrary definitions of quorums
Ally Consensus

Consensus servers link to library and provide application-independent agreement.

Applications link to library to access protocol for proposing and listening.

Separated application and agreement has been shown advantageous.

Increased fault tolerance from threshold cryptography.
Ally Consensus

Consensus servers link to library and provide application-independent agreement

Applications link to library to access protocol for proposing and listening

Separated application and agreement has been shown advantageous

Increased fault tolerance from threshold cryptography
Ally Consensus

Consensus servers link to library and provide application-independent agreement.

Applications link to library to access protocol for proposing and listening.

Separated application and agreement has been shown advantageous.

Increased fault tolerance from threshold cryptography.
Ally Consensus

Consensus servers link to library and provide application-independent agreement

Applications link to library to access protocol for proposing and listening

Separated application and agreement has been shown advantageous

Increased fault tolerance from threshold cryptography
Ally Consensus

Consensus servers link to library and provide application-independent agreement.

Applications link to library to access protocol for proposing and listening.

Separated application and agreement has been shown advantageous.

Increased fault tolerance from threshold cryptography.
Future Work

Generalize threshold to distributed cryptography

Generalize notion of quorum and provide management

Provide higher-level application-building abstractions
Future Work

Generalize threshold to distributed cryptography

Generalize notion of quorum and provide management

Provide higher-level application-building abstractions
Future Work

Generalize threshold to distributed cryptography

Generalize notion of quorum and provide management

Provide higher-level application-building abstractions
**Future Work**

Generalize threshold to distributed cryptography

Generalize notion of quorum and provide management

Provide higher-level application-building abstractions